2020

# Hardware-in-the-Loop CPS Security Architecture for DER Monitoring and Control Applications

Ravikumar Gelli
*Iowa State University*, gelli@iastate.edu

Burhan Hyder
*Iowa State University*, bhyder@iastate.edu

Manimaran Govindarasu
*Iowa State University*, gmani@iastate.edu

# Hardware-in-the-Loop CPS Security Architecture for DER Monitoring and Control Applications


## Abstract

Deeper penetration of interoperable cyber-physical distributed energy resources (DER) and their utility-wide remote monitoring and control drastically increases cybersecurity attack surface. Utilities require to adopt the DER interconnection and communication standards to a range of autonomous, advanced and curve-based grid-support functions to securely monitor and control DER devices for ensuring power quality, voltage, and system frequency. In this paper, we present DER monitoring and control (DERMC) cyber-physical system (CPS) architecture including standard communication protocols such as IEEE 2030.5 [1] and discuss various stealthy cyber attack vectors that affect communications and operations of DER. We propose a hardware-in-the-loop (HIL) CPS security architecture and testbed design with industry-grade software and hardware systems and a real-time digital simulator for high-fidelity grid impact characteristic analysis against cyber attack vectors. We use the testbed to demonstrate impact characteristics for modified IEEE 13 bus system including 11 solar photovoltaic units. The experiments demonstrated significant results by 100% real-time performance and zero overruns.



## Keywords

CPS security, Distributed energy resource, DER monitoring and control, DER communications, Hardware-in-the-loop testbed, Smart distribution grid


## Disciplines

Power and Energy


## Comments

This is a manuscript of a proceeding published as Ravikumar, Gelli, Burhan Hyder, and Manimaran Govindarasu. "Hardware-in-the-Loop CPS Security Architecture for DER Monitoring and Control Applications." In *2020 IEEE Texas Power and Energy Conference (TPEC).* (2020). DOI: 10.1109/TPEC48276.2020.9042578. Posted with permission.

# Hardware-in-the-Loop CPS Security Architecture for DER Monitoring and Control Applications

Gelli Ravikumar, *Member, IEEE*, Burhan Hyder, *Student Member, IEEE*, Manimaran Govindarasu, *Fellow, IEEE*

***Abstract*—Deeper penetration of interoperable cyber-physical distributed energy resources (DER) and their utility-wide remote monitoring and control drastically increases cybersecurity attack surface. Utilities require to adopt the DER interconnection and communication standards to a range of autonomous, advanced and curve-based grid-support functions to securely monitor and control DER devices for ensuring power quality, voltage, and system frequency. In this paper, we present DER monitoring and control (DERMC) cyber-physical system (CPS) architecture including standard communication protocols such as IEEE 2030.5 [1] and discuss various stealthy cyber attack vectors that affect communications and operations of DER. We propose a hardware-in-the-loop (HIL) CPS security architecture and testbed design with industry-grade software and hardware systems and a real-time digital simulator for high-fidelity grid impact characteristic analysis against cyber attack vectors. We use the testbed to demonstrate impact characteristics for modified IEEE 13 bus system including 11 solar photovoltaic units. The experiments demonstrated significant results by 100% real-time performance and zero overruns.**

***Index Terms*—CPS security, Distributed energy resource, DER monitoring and control, DER communications, Hardware-in-the-loop testbed, and Smart distribution grid.**

## I. Introduction

SECURE , reliable, and resilient operation of the modern cyber-physical power system including high penetration of renewable resources is of paramount importance and critical for the power utilities. The proliferation and widespread availability of cost-effective Distributed Energy Resources (DERs) in electric distribution systems present many challenges and opportunities for utilities on the planning and reliable operation of the active distribution grid. The increasing prevalence of DER cyber-physical systems (CPS) and their common-mode vulnerabilities may lead to cyber-threats and risk of detaching substantial generation during peak demand. It could cause power disruptions and instability in the grid operation. While a traditional cyberattack on information technology (IT) systems may leak credit-card or other sensitive information, a CPS attack can lead to a loss of situational awareness and control in the power grid, DERs, reactors, gas turbines, and other critical infrastructure. Therefore, it becomes a significant requirement to establish secure monitoring and control of DERs by integrating cyber defensive strategies to ensure reliable active distribution grid operation against cyber attacks. It is more pronounced and essential to build cyber-secure infrastructure for real-time monitoring, control, and optimization of DERs to cope with variability and bidirectional power flows.

Gelli Ravikumar, Burhan Hyder and Manimaran Govindarasu are with the Department of Electrical and Computer Engineering, Iowa State University, USA. (e-mail: gelli@iastate.edu, bhyder@iastate.edu, and gmani@iastate.edu)

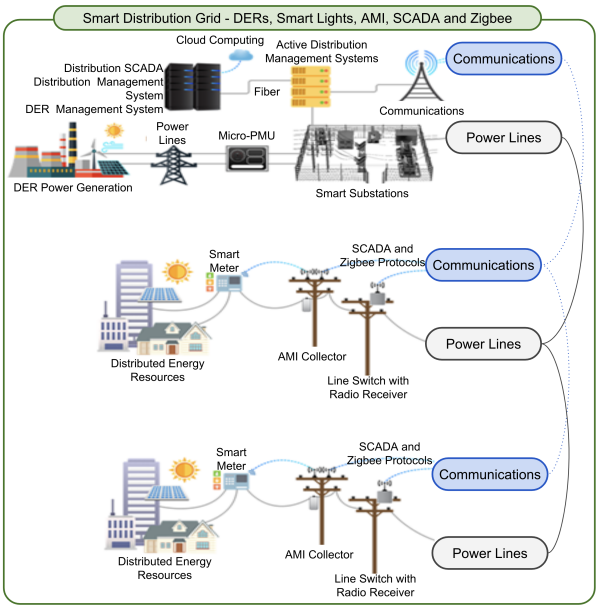


Fig. 1. Cyber-Physical Smart Distribution Grid including DERs

Fig. 1 shows a schematic of cyber-physical smart distribution grid including DERs. Increasing penetration of DER devices such as solar photovoltaic (PV), wind, battery energy storage systems (BESS), electric vehicles (EV), and EV charging stations (EVCS) in distribution networks expands the cyber-attack surface and demands stringent requirements to establish highly-secured communications. As the DER devices are becoming cyber-physical systems and entering the broader realm of the Internet of Things, early susceptibility to cyber threats have been observed. For example, a PV device was exposed to threats when adversaries attempted to gain access via a compromised VPN tunnel connected to the Field Area Network of a DC optimizer data manager [2]. A European PV inverter manufacturer discovered over a dozen vulnerabilities, including remote access vulnerabilities that could compromise the PV equipment [3]. Traditional cybersecurity technologies can have substantial false-positives and false-negatives with the continuous expansion of networked DER devices [4], [5], which could significantly impact grid operation. There is an urgent need to develop innovative defense-in-depth strategies, state-of-the-art cyber-security practices for solar PV systems, DERs, aggregators, and utility grid operators for attack resilient and reliable operation of the U.S. power system [6].

To address these cybersecurity challenges and to incorporate grid-support functions, power utilities and system operators at different levels (ISOs/TSOs/DSOs) are upgrading their systems compliant to the DER interconnection standards including grid-support advanced functions in the United States [7] and world-wide [8]. Some large-scale investor-owned DER

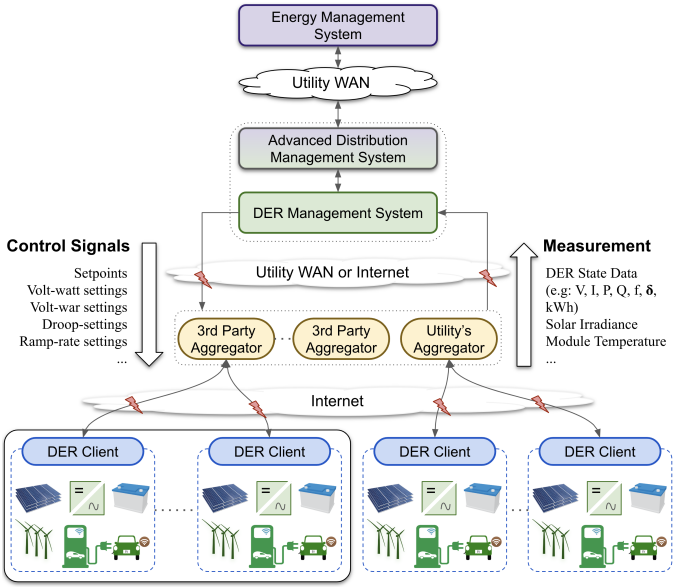


Fig. 2. Proposed DER Monitoring and Control Architecture including ADMS, EMS, and Cyber Attack Surface

plants and utility-scale DER plants connect to utility operators via fiber-optic lines, telephone lines, cellular modems, and other radio relays, so there are several access points to these systems [6]. Recent projects on cybersecurity for DER [9]–[11] have attempted to explore device-centric and protocol-centric cybersecurity properties and devise algorithms for securing DER devices integrated to the grid. These methodologies may fail to provide adequate cybersecurity as the number of DER devices increase in the grid operation. Therefore, it is essential to develop a comprehensive CPS security analysis for DERs using industry-grade software and hardware systems to test and evaluate the cyber attack-defense algorithms. As the subject of this paper, we present a cyber-physical DER architecture and hardware-in-the-loop CPS testbed design including real-time digital simulator, DER clients, aggregator, DER utility server, and DERMS. The proposed DER CPS testbed system is integrated with the existing CPS security smart grid testbed [12] for the grid impact characteristics.

## II. Proposed DER Monitoring and Control Architecture

Fig. 2 shows the proposed CPS control loop architecture for the DER monitoring and control applications. The CPS of DERs employed with different DER communication protocols enable utility distribution system operators to centrally monitor and control in real-time and provide performance and state of the DER devices to the associated prosumers. The DER monitoring and control of the geographically distributed devices provide greater flexibility for system operators to ensure efficient and stable grid operation, but, it drastically increases the cyber attack surface of the DER integrated power grid.

As it is practically difficult to control each DER device, the DER communication standards propose aggregation of various geographically distributed devices, where the aggregation of a group of DER devices forms distributed virtual power plant. To optimally and efficiently address the grid requirements, the standards recommend to form the group-wise DER controls. A possible scenario of the hierarchical configuration of groups defined in common smart inverter profile (CSIP). Although the aggregation of DER system provide flexibility to control the set-points in response to the grid operation, it may increase the attack surface as hostile entities can access the DER devices remotely through the aggregator systems and affect multiple systems, state variables, and dynamics of the grid. Moreover, as the CPS infrastructure enables monitoring, control, and reconfiguration of DER devices such as smart inverter units, adversaries may exploit and gain access to the DER devices remotely and manipulate their operation. Therefore, it is essential to deploy advanced cyber-defense mechanisms to provide a CPS-aware situational awareness and anomaly detection so that model-base mitigation strategies can be employed.

TABLE I
Smart Inverter Functions

| Immediate Controls | Curve Controls |
|---|---|
| Active Power set point (opModFixedFlow) | Voltage-VAr curve (opModVoltVAr) |
| Power Factor set point (opModFixedPF) | Volt-Watt curve (opModVoltWatt) |
| Reactive Power set point (opModFixedVAr) | Frequency-Watt curve (opModFreqWatt) |
| Maximum Active Power output limit (opModMaxLimW) | Watt-Power Factor curve (opModWattPF) |
| Connect/Disconnect (opModConnect) | Ride Through:<br>High voltage disturbance response curve (opModHVMustTrip)<br><br>High voltage momentary cessation disturbance response curve (opModHVMomentaryCessastion)<br><br>Low voltage must trip disturbance response curve (opModLVMustTrip)<br><br>Low voltage momentary cessation disturbance response curve (opModLVMomentaryCessastion) |
| Energize/De-energize (opModEnergize) | Trip:<br>High frequency must trip disturbance response curve (opModHFMustTrip)<br><br>Low frequency must trip disturbance response curve (opModLFMustTrip) |
| Active Power set point in Watts (opModTargetW) | |
| Reactive Power set point in VARs (opModTargetVAr) | |

TABLE II
Attack vectors and their impacts on DER Systems

| Attack Type | Attack Target | Impact |
|---|---|---|
| Data Integrity Attacks | Control Signals<br>Measurement Signals | Poor Power Quality,<br>Voltage Instability,<br>Generation Loss |
| DoS Attack | Aggregators<br>DER Client devices | Loss of Situational Awareness,<br>Generation Imbalance |
| Malware Injection Attacks | PV Controller Firmware | Inefficient Operation of PV Modules,<br>Frequency Instability |
| Coordinated attacks: Data Integrity + DDoS Attacks | Control Signals<br>Measured Signals<br>Aggregators<br>DER Client devices | Generation Loss,<br>Frequency Instability<br>Voltage Instability,<br>PV Plant Outage |

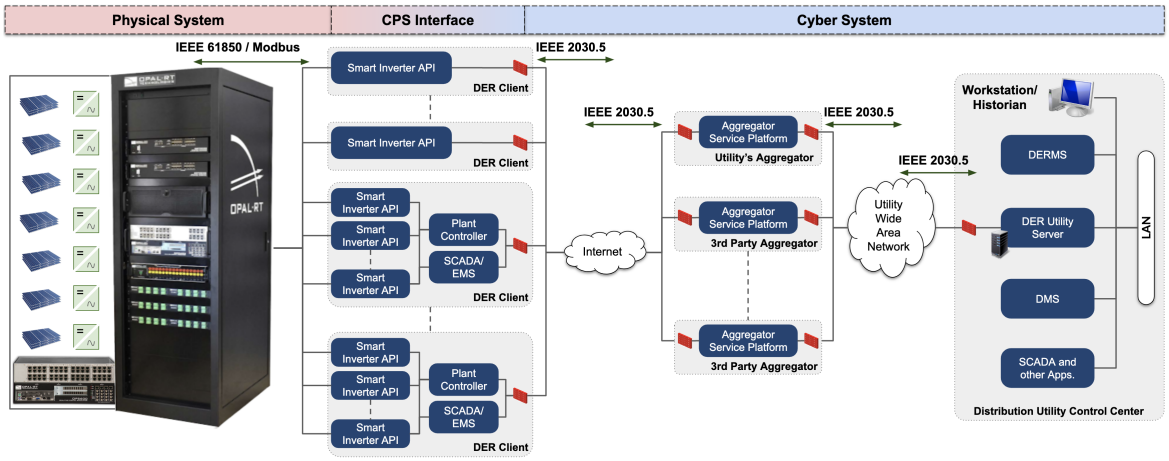


Fig. 3. Proposed Hardware-in-the-Loop DER CPS Security Testbed Design and Architecture

### A. CPS Control Loop

Fig. 2 shows the proposed CPS control loop architecture for the DER systems for remote monitoring and control applications. At the utility control center, the Distributed Energy Resource Management System (DERMS) receives measurements and sends control commands over the utility wide-area network from the geographically distributed aggregator software systems. The aggregators can be utility-owned or third-party-owned software systems, which can usually be deployed at a private cloud, public cloud, or utility control center premises. The DER plant controllers, referred to as DER clients, send and receive signals to and from the third-party aggregators or utility's aggregator. We consider utility's aggregator software system to provide the functionality for the direct communication between the DER clients and DERMS scenario. The DERMS, which receives data from the Advanced Distribution Management System (ADMS), the Energy Management System (EMS), and the DER plant controllers or aggregators, prepares control signals such as voltage and frequency setpoints, frequency droop and active power ramp-rate settings, and automated generation control signals and sends them to the DER plant controllers via the WAN. The DERMS receives various measurements from the PV plant controllers over the DER-WAN such as plant state data including voltage, active and reactive power output, frequency, power factor, and energy output, irradiance being received by the PV modules, and the temperature of the modules.

As shown in the architecture, the possibility of cyber attacks can occur either at the tier-1, tier-2 or both. The tier-1 communication is between the DER clients and aggregator software systems. The tier-2 communication is between the aggregators and DERMS. The California rule-21 and CSIP recommends utility controlled cybersecurity at the tier-2 level. The possible cybersecurity strategies include virtual private networking (VPN) between the utility communication server and each of the aggregator software systems.

### B. DER System Operation and Functions

Table I shows the functions that a smart DER device such as a smart inverter is capable of carrying out. These functions include the Immediate Controls and the Curve Controls. Immediate controls can be either in the default mode or the event-triggered mode. In the default mode, the smart device follows the default function settings while in the event-triggered mode, special functions related to the specific predefined events that occur in the grid are triggered. The curve controls are functions that are specific to the system operation. Table I lists down some of these functions with regards to a smart inverter as per California rule-21.

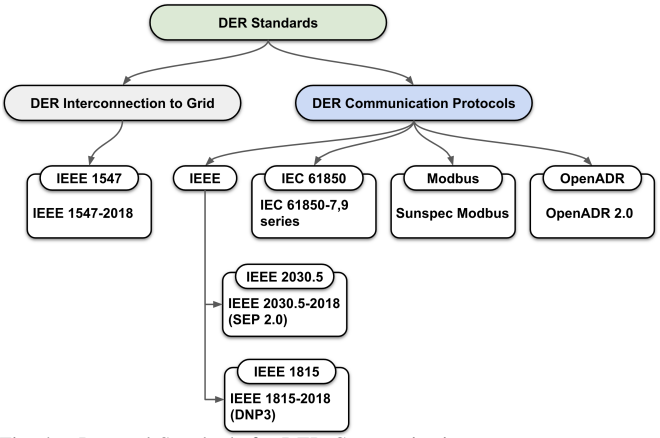


Fig. 4. Protocol Standards for DER Communication

### C. Stealthy Cyber attack Vectors and Impacts

Table II shows a brief overview of various cyberattacks and their impacts that the existing Solar PV systems are susceptible to. The attacks include: data integrity attacks, Denial of Service attacks, timing attacks, replay attacks, or other forms of man-in-the-middle attacks. These attacks can be targeted on the measurement signals or control signals. In addition, sophisticated attacks include coordinated cyber attacks that target multiple control loops (sensing and control) simultaneously. Any successful attack may have negative impacts on the DERs and DER integrated distribution grid system and hence the transmission system depending on the capacity of the solar power plant, magnitude and location(s) of the attacks.

## III. Proposed HIL CPS Testbed Architecture

Fig. 3 shows the HIL CPS testbed implementation architecture including the selected DER communication protocols for

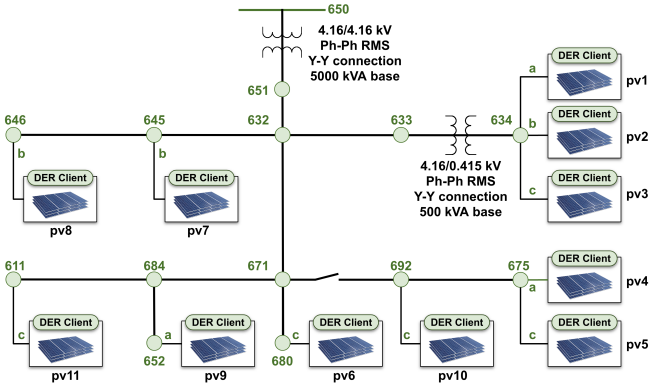


Fig. 5. Modified IEEE 13 Bus Distribution Grid with Integration of PVs

| PV | Bus | P_gen (p.u.) | Q_gen (p.u.) | Vt_abs (p.u.) | Vt_ang (deg) | P_max (p.u.) |
|---|---|---|---|---|---|---|
| pv1 | 634_a | 0.15 | 0.1 | 1 | -121.9 | 0.2 |
| pv2 | 634_b | 0.1 | 0.09 | 1 | -122 | 0.2 |
| pv3 | 634_c | 0.1 | 0.05 | 1 | 115 | 0.2 |
| pv4 | 675_a | 0.5 | 0.2 | 1 | -5.9 | 1 |
| pv5 | 675_c | 0.3 | 0.2 | 1 | 115 | 0.5 |
| pv6 | 680_c | 0.5 | 0.2 | 1 | 115.2 | 1 |
| pv7 | 645_b | 0.2 | 0.14 | 1 | -121.9 | 0.5 |
| pv8 | 646_b | 0.25 | 0.15 | 1 | -122 | 0.5 |
| pv9 | 652_a | 0.15 | 0.1 | 1 | -5.9 | 0.2 |
| pv10 | 692_c | 0.2 | 0.15 | 1 | 115.2 | 0.5 |
| pv11 | 611_c | 0.2 | 0.1 | 1 | 115 | 0.5 |

Fig. 6. Specifications for individual PV modules

monitoring and controlling the DER devices. The significant components of the HIL CPS testbed include - 1) Real-time digital simulator module: It emulates characteristics for DER devices such as solar PV. 2) DER client module: It consists of smart inverter application programming interface (API) to receive and send signals to the DER devices via Modbus or IEC 61850 protocol. The DER client module also includes plant-wide SCADA/EMS software system to monitor and control a group of smart inverter APIs. 3) Aggregator module: These are two-fold – a) Utility-owned aggregator software system and b) Third-party-owned aggregator software system. These will acts as servers to the DER client under the tier-1 communication, and clients to the utility server under the tier-2 communication. 4) DER utility server module: It communicates to the aggregator modules via DER communication protocols such as IEEE 2030.5 [1] and exchange information across the the DERMS, DMS, EMS, SCADA and other distribution control center applications. 5) DERMS module: It is the signification module to conduct analysis on the distribution grid systems and populate required grid-support functions as stated in the Section II. The DERMS module interacts with the DER utility server to receive and send signals from and to the DERs.

### A. DER Communication Scenarios

There are primarily four communication scenarios exist between the DER utility server and DER clients are - 1) Direct communication between utility provider (utility's aggregator) and DER client, 2) Direct connection between utility provider (utility's aggregator) and large-scale DER client comprising of generation facility EMS, 3) Indirect communication between utility provider and DER client through a third-party aggregator, and 4) A mutual agreement based communication between utility and DER client

| PV | TIME1 (sec) | IRRADIANCE1 (W/m^2) | TIME2 (sec) | IRRADIANCE2 (W/m^2) | TIME3 (sec) | IRRADIANCE3 (W/m^2) | TIME4 (sec) | IRRADIANCE4 (W/m^2) | TIME5 (sec) | IRRADIANCE5 (W/m^2) | TIME6 (sec) | IRRADIANCE6 (W/m^2) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| pv1 | 1 | 700 | 5 | 800 | 8 | 1000 | 12 | 1100 | 15 | 800 | 20 | 600 |
| pv2 | 1 | 400 | 5 | 500 | 8 | 700 | 12 | 800 | 15 | 500 | 20 | 300 |
| pv3 | 1 | 400 | 5 | 500 | 8 | 700 | 12 | 800 | 15 | 500 | 20 | 300 |
| pv4 | 1 | 400 | 5 | 500 | 8 | 700 | 12 | 800 | 15 | 500 | 20 | 300 |
| pv5 | 1 | 600 | 5 | 700 | 8 | 900 | 12 | 1000 | 15 | 700 | 20 | 500 |
| pv6 | 1 | 400 | 5 | 500 | 8 | 700 | 12 | 800 | 15 | 500 | 20 | 300 |
| pv7 | 1 | 333.3333333 | 5 | 433.3333333 | 8 | 633.3333333 | 12 | 733.3333333 | 15 | 433.3333333 | 20 | 233.3333333 |
| pv8 | 1 | 400 | 5 | 500 | 8 | 700 | 12 | 800 | 15 | 500 | 20 | 300 |
| pv9 | 1 | 700 | 5 | 800 | 8 | 1000 | 12 | 1100 | 15 | 800 | 20 | 600 |
| pv10 | 1 | 333.3333333 | 5 | 433.3333333 | 8 | 633.3333333 | 12 | 733.3333333 | 15 | 433.3333333 | 20 | 233.3333333 |
| pv11 | 1 | 333.3333333 | 5 | 433.3333333 | 8 | 633.3333333 | 12 | 733.3333333 | 15 | 433.3333333 | 20 | 233.3333333 |

Fig. 7. Time varying irradiance values received by individual PV modules

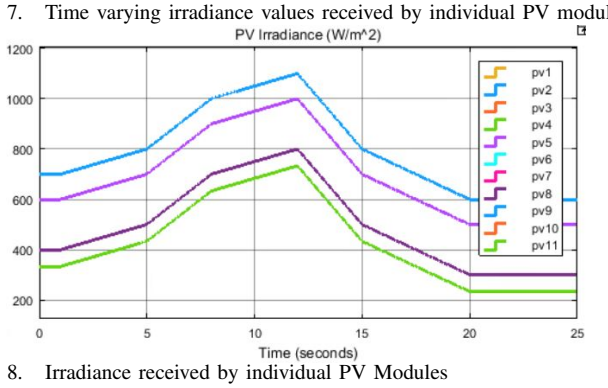


Fig. 8. Irradiance received by individual PV Modules

### B. DER Communication Protocols

Fig. 4 shows the hierarchy of DER standard protocols. IEEE 1547 is used for the DER interconnection to the grid. There are five active standards for the DER communication between the geographically distributed DER devices and utility.

## IV. Case Study

Fig. 5 shows the modified IEEE 13-bus distribution grid that we used for the case study. It has 14 buses including the bus (650) that integrates the distribution grid to the main grid. There are a total of 11 PV modules that are connected to the various nodes. PV modules connected to Node 634 are operating at $0.415kV$ and the rest of the PV modules operate at $4.16kV$. The following modifications were made to the IEEE 13-bus distribution grid in for this case stude: 1) PV units were connected to buses 634, 675, 692, 680, 652, 611, 646, and 645; 2) The distributed load along the line 632 to 671 was replaces by a lumped load a bus 632; 3) The voltage regulator between nodes 632 and 650 was substituted by a transformer (Yg-Yg), and a new node 651 was inserted; and 4) All were considered with grounded star (Yg) concoction.

The specifications of all the PV modules are given in the table in Fig. 6. It shows the PV modules names; the buses that the respective modules are connected to; the active and reactive power generated by the modules; the terminal voltage magnitudes and angles of the PV modules; and the maximum rated active power generation for each module. Each PV unit model is based on the PSS/e Photovoltaic System Model and includes a converter model (PVGU1), a controller (PVEU1), a solar panel (PANELU1), and an irradiance model (IRRADU1). Real-time simulation of this grid was carried out on OPAL-RT real-time digital simulator to capture the dynamics of the microgrid. To simulate the phenomena of sunrise and sunset on a shorter timescale of 25 seconds, an irradiance profile as depicted in Fig. 7 was considered. The irradiance profile shows that irradiance for all modules first increases starting at $TIME1$ up to $TIME4$ and then starts to decrease from

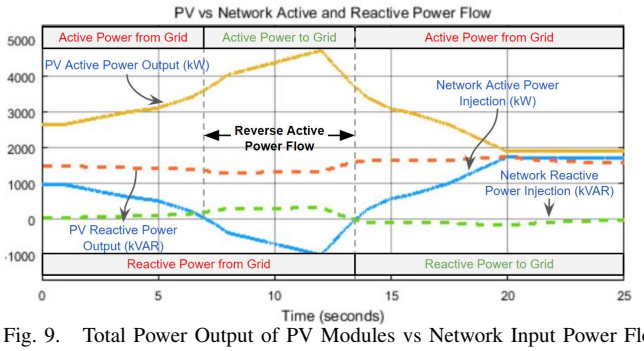


Fig. 9. Total Power Output of PV Modules vs Network Input Power Flow

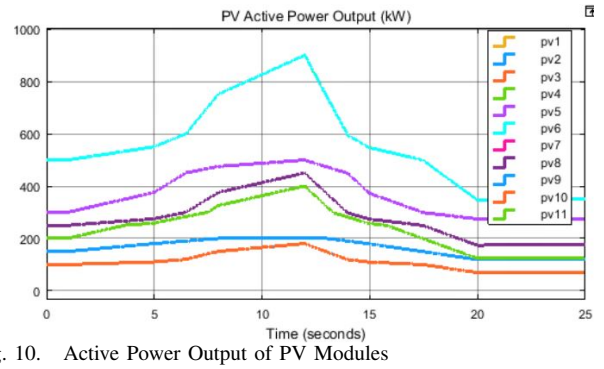


Fig. 10. Active Power Output of PV Modules

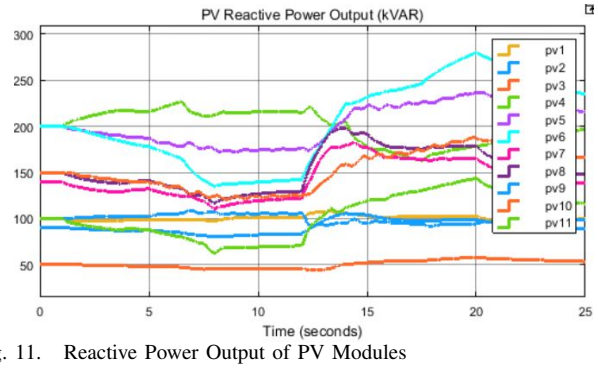


Fig. 11. Reactive Power Output of PV Modules

| Probes | Info | | | |
|---|---|---|---|---|
| | Usage [%] | Min | Max | Mean |
| phasor18_MicroGrid Ts=0.01[s] | 4.4% | | | |
| sm_master Ts...9776482582[s] | 4.4% | dt= 403.20 [us] | dt= 492.25 [us] | dt= 439.71 [us] |
| New data acquisition | 0.0% | dt= 0.27 [us] | dt= 0.35 [us] | dt= 0.30 [us] |
| Major computation time | 4.36% | dt= 399.16 [us] | dt= 488.22 [us] | dt= 435.60 [us] |
| Minor computation time | 0.0% | dt= 0.38 [us] | dt= 0.43 [us] | dt= 0.40 [us] |
| Execution cycle | 4.4% | dt= 403.20 [us] | dt= 492.25 [us] | dt= 439.71 [us] |
| Total step size | 100.0% | dt= 10000.28 [us] | dt= 10002.62 [us] | dt= 10001.64 [us] |
| Total idle | 95.58% | dt= 9504.79 [us] | dt= 9595.35 [us] | dt= 9557.79 [us] |

Fig. 12. Real-Time Digital Simulator OPAL-RT CPU usage

$TIME5$ up to $TIME6$, having the lowest irradiance levels at $TIME6$, that is, after 20 seconds of simulation time. Fig. 8 depicts the same irradiance information on a graph for all PV modules. Fig. 9 shows the total active and reactive power generated by the PV modules and the active and reactive power injected by the main grid into the microgrid. The graph clearly shows that the active power generated by the PV modules reaches its maximum around 12 seconds when the irradiance is also maximum and reaches its minimum value around 20 seconds when the irradiance is also minimum. When the PV module active power output is maximum, the active power injection into the microgrid is minimum. In fact, the there is a reverse active power flow from the microgrid to the main grid from approximately 8 seconds to 13 seconds. The reactive power output from the PV modules flows from the microgrid to the main grid from around 13 seconds right after the reverse active power flow ends. Fig. 10 and 11 show the active and reactive power output for all the PV modules.

Fig. 12 shows the CPU usage for the real-time digital simulation of the distribution grid model on OPAL-RT. With a time step of 10 milliseconds, the CPU uage is only $4.4\%$ having a mean computation time of $439.71$ microseconds and the CPU remaining idle for $95.58\%$ of the time

## V. Conclusion

We proposed a high-fidelity HIL CPS security testbed architecture and design for grid impact characteristic analysis against various cyber attack vectors with industry grade software and hardware systems. We have conducted an experiment on a modified IEEE 13 bus distribution grid with 11 PV modules and demonstrated $100\%$ real-time performance and zero overruns for a time step of 10 milliseconds and $4.4\%$ CPU usage of $439.71$ microseconds. The proposed testbed architecture provides grid impact characteristics for integration of DER in the smart grid with high-fidelity which is indispensable for the development and testing of new tools and technologies for cybersecurity in the DER integrated-grid.

## VI. Acknowledgement

This research is funded in part by US NSF Grant # CNS 1446831 and US DOE Grant # DE-EE0008773.

## References

[1] IEEE 2030.5, *IEEE 2030.5-2018 - IEEE Standard for Smart Energy Profile Application Protocol*. Edition 1.0, December 2018.

[2] F. Bret-Mounet, "All your solar panels are belong to me," *DEF CON*, vol. 24, pp. 4–7, 2016.

[3] H. Scenario, "Exploiting a weak spot in the power grid," 2019. [Online]. Available: https://horusscenario.com/

[4] D. J. Sebastian and A. Hahn, "Exploring emerging cybersecurity risks from network-connected der devices," in *2017 North American Power Symposium (NAPS)*, Sep. 2017, pp. 1–6.

[5] J. Qi, A. Hahn, X. Lu, J. Wang, and C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Physical Systems: Theory Applications*, vol. 1, no. 1, pp. 28–39, 2016.

[6] Lai, Christine and Jacobs, Nicholas and Hossain-Mckenzie, Shamina and Carter, Cedric and Cordeiro, Patricia and Onunkwo, Ifeoma and Johnson, Jay, "Sand2017-13113: Cyber security primer for der vendors, aggregators, and grid operators," December 2017.

[7] Sunspec, "Common smart inverter profile: Ieee 2030.5 implementation guide for smart inverters," 2018. [Online]. Available: https://sunspec.org/wp-content/uploads/2018/04/CSIPImplementationGuidev2.103-15-2018.pdf

[8] R. Bründlinger, "Advanced smart inverter and der functions requirements in latest european grid codes and future trends," 12 2015.

[9] Colin Dunn, "Low-cost, plug-and-play data diodes for solar equipment cybersecurity," 2018. [Online]. Available: https://www.sbir.gov/sbirsearch/detail/1523325

[10] J. Coignard, T. Nouidui, C. Gehbauer, M. Wetter, J. Joo, P. Top, R. R. Soto, B. Kelley, and E. Stewart, "Cyder - a co-simulation platform for grid analysis and planning for high penetration of distributed energy resources," in *IEEE PESGM*, Aug 2018, pp. 1–5.

[11] Robert Goldman, "Solar guard," 2018. [Online]. Available: https://www.sbir.gov/sbirsearch/detail/1524179

[12] Gelli Ravikumar, Burhan Hyder, and Manimaran Govindarasu, "Efficient modeling of hil multi-grid system for scalability & concurrency in cps security testbed," in *NAPS*, Oct 2019.